NBSIR 75-909

# Index of Automated System Design Requirements as Derived from the OMB Privacy Act Implementation Guidelines

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

October 1975

Final



U S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 75-909

# INDEX OF AUTOMATED SYSTEM DESIGN REQUIREMENTS AS DERIVED FROM THE OMB PRIVACY ACT IMPLEMENTATION GUIDELINES

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234



October 1975

Final

U.S. DEPARTMENT OF COMMERCE, Rogers C.B. Morton, *Secretary*
James A. Baker, III, *Under Secretary*
Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

## Foreword

This index is a list of certain requirements which must be considered by Federal technical and administrative personnel in order to comply with those provisions of the Privacy Act of 1974* relating to automated systems design and development. This index has been derived from the Office of Management and Budget (OMB) guidelines** for implementing those provisions. Each requirement listed contains a reference to an applicable part of the Privacy Act and to a page and column number of the OMB guidelines as they appear in the Federal Register. Therefore, these documents must be used in conjunction with this index. Furthermore, a familiarity with these documents will increase the utility of this index.

This document was prepared within the Federal Information Processing Standards Task Group 15. This task group was established by the Department of Commerce within its National Bureau of Standards to develop standards and guidelines in Computer Systems Security. Special recognition should go to the following participants of the task group which has commended their efforts in preparing this document: Margaret W. Alter, Office of Federal Management Policy, General Services Administration; Philip H. Diamond, Department of Data Management, Veterans Administration; and Robert H. Follett, Office of Federal Business Relations, International Business Machines Corporation.

Any comments you have concerning this index or its use are welcomed. Please forward them to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234, or telephone (301) 921-3157.

---

* Privacy Act of 1974; Public Law 93-579.

** Privacy Act Implementation Guidelines and Responsibilities, Office of Management and Budget, dated July 1, 1975 and published in the Federal Register on July 9, 1975 (40 FR 28947-28978).

# INDEX OF AUTOMATED SYSTEMS DESIGN REQUIREMENTS DERIVED FROM THE JULY 1, 1975, OMB PRIVACY ACT GUIDELINES *

## I. Technical Requirements

### A. Systems Design Requirements

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28966 | 1 | 3(e)(10)** | 1. Agencies must provide adequate technical, physical and administrative safeguards to protect data from unauthorized alteration or disclosure. |
| 28954 | 1 | 3(b)(1) | 2. Agencies must impose some constraints on the transfer of records to assure that recipients of data within the agency have an official "need to know". |
| 28958<br>28960<br>28961 | 3<br>2-3<br>1 | 3(d)(2)(B)<br>3(e)(1) | 3. Only relevant and necessary information should be maintained. Agencies shall assess the legality of, need for, and relevance of the information to agency purposes whenever any change is proposed in a system of records, when a system is designed and developed, when public notices are written, when requests to delete information are received from data subjects, and at least annually as part of a regular program of the agency's record-keeping practices. |
| 28961 | 1 | 3(e)(1) | 4. Whenever using or disclosing any individual records the content of the records shall be examined to ensure that the information is both relevant and necessary. |
| 28960<br>28965 | 3<br>2-3 | 3(e)(1)<br>3(e)(7) | 5. A list of the types of questions the agency shall consider when determining whether information is both "relevant and necessary" is provided in the guidelines. |
| 28961 | 1-3 | 3(e)(2) | 6. Agencies must collect information directly from the individual to the greatest extent possible when the information may be used to make an adverse determination about that individual. |
| 28961 | 2 | 3(e)(2) | 7. A list is provided of the points an agency should consider when it intends to collect information from third-party sources. |
| 28961 | 3 | 3(e)(3) | 8. When collecting information the agency must tell the individual why the information is collected - i.e., collect the information only with the individual's informed consent. |

* "Privacy Act Guidelines", Federal Register, Wednesday, July 9, 1975, Vol. 40, No. 132, PP 28947-28978.

**See also FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, Inst. for Computer Sciences and Technology, NBS, May 30, 1975.

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28961 | 3 | 3(e)(3) | 9. When the agency collects information from third-party sources, the sources should be informed of the purposes for which the information will be used. |
| 28954<br>28952 | 3<br>3 | 3(b)(5)<br>3(a)(6) | 10. There must be provisions to strip records of individual identifiers so that the identities of individuals cannot be discerned when statistical research or reporting records are disclosed or transferred. |
| 28954 | 3 | 3(b)(5) | 11. Provisions must also exist for ensuring that an individual's identity cannot be discerned from tabulations or other presentations of statistical data by combining various statistical records or referring to other available information. |
| 28956<br>28957 | 3<br>1-3 | 3(d)(1) | 12. Records must be shown to the individual in a form that is comprehensible to him or her. "Whenever possible... the requested record should be made available in the form in which it is maintained by the agency and the extraction or translation process may not be used to withhold information..." |
| 28957<br>28951<br>28952 | 1<br>3<br>1 | 3(d)(1)<br>3(a)(4)<br>3(a)(5) | 13. The agency is not required to grant the individual access to information about himself when it is not retrieved by the individual's name or other identifier. The Act "gives an individual the right of access only to records which are contained in a system of records". (See definitions of "record" and "system of records" in OMB Guidelines.) |
| 28964<br>28967 | 2<br>1 | 3(e)(4)(G)<br>3(f)(1) | 14. The agency must be able to answer the following questions:<br>a. What information should the individual give the agency when the individual doesn't know the retrieval code assigned to him or her for a particular system of records?<br>b. What information should the individual give the agency if records are currently retrieved by Social Security Number (SSN) and the individual refuses to give the agency that number?* |
| 28957<br>28967 | 2<br>1 | 3(d)(1)<br>3(f)(1) | (The agency cannot refuse to grant individuals access to records about themselves for refusing to disclose their SSN's even when the SSN is used to retrieve their records.) |
| 28967 | 1 | 3(f)(1) | 15. The agency has to be able to retrieve records about individuals when individuals do not know the particular retrieval code assigned to themselves for a given system or records. |

See Comment on Page 4

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28967 | 1 | 3(f)(1) | 16. The development of new retrieval and indexing capabilities to comply with provisions listed in items 13-15 above is not encouraged. The use of existing capabilities is. |
| 28955 | 2 | 3(b)(8) | 17. Agencies must be able to retrieve records that could be crucial to the health or safety of an individual without the consent of the individual to whom the records pertain. |
| 28955 | 2-3 | 3(b)(8) | 18. The agency must transmit a notice of disclosure to the last known address of the individual whose record is disclosed when the record is disclosed in an emergency and when the delay of disclosure could affect the health or safety of any individual. |
| 28965 | 3 | 3(e)(8) | 19. The agency must notify the individual at his or her last known address if the record is disclosed under compulsory legal process when the issuance of the legal order is made public. The agency must make an accounting of the disclosure at the time the agency complies with the order or subpoena. (No separate address record is required.) |
| 28957<br>28961 | 3<br>3 | 3(d)(1)<br>3(e)(3) | 20. It may be necessary to extract required information from records- (for example: (1) If access to an entire document might disclose information about individuals that is not relevant to the request; (2) if access might reveal the identities of sources of information who were guaranteed confidentiality.) |
| 28963 | 1 | 3(e)(4) | 21. "Systems ... should not be subdivided or reorganized so that information which would otherwise have been subject to the act is no longer subject to the act." |
| 28965<br>28964 | 1<br>3 | 3(e)(6)<br>3(e)(5) | 22. Records must be accurate, relevant, timely and complete for agency purposes at the time of dissemination and when making determinations regarding the individual. (Agencies may develop tolerances for "accuracy" and "timeliness" keeping in mind the likelihood and consequences of error.) |

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | | |
|---|---|---|---|---|
| 28958<br>28967 | 2<br>3 | 3(d)(2)(B)<br>3(f)(4) | 23. | Agencies must be able to amend all data elements that pertain to the individual. |
| 28958 | 2-3 | 3(d)(2)(B) | 24. | Design considerations should include the deletion of data at the request of the individual. Requests for deletion of data should be handled in accordance with procedures established by the agency for amending records at the individual's request. |
| 28959<br>28960 | 2-3<br>1 | 3(d)(3)<br>3(d)(4) | 25. | Statements of dispute need not be maintained as an integral part of the record to which they pertain. However, a special indicator on an entire automated record or an indicator specific to the portion in dispute should be included in records about which the contents are disputed so that the statements of dispute can be disclosed along with the record. |
| 28960 | 1 | 3(d)(4) | 26. | Agencies may include a brief summary of their reasons for not making a correction when disclosing disputed information. This statement will be given to the individual whenever he or she requests access to the record. |

*Comment; Individuals can refuse to disclose their SSN's except in those cases where;

(1) disclosure of SSN is required by Federal statute, or
(2) the system of records from which information is to be retrieved requires disclosure of SSN as a means of verifying an individual's identity, and the system was in existence and operating before January 1, 1975, and the statutes or regulations which require such disclosure were adopted before January 1, 1975.

B. Requirements Affecting Forms Design

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28962 | 1 | 3(e)(3)(A) | 27. The agency should try to collect required and optional information on separate forms because the effect of including both types of information on the same form is likely to be coercive on some respondents. (It follows from this requirement that control codes would have to be established to link separate forms for processing.) |
| 28961 | 3 | 3(e)(3) | 28. When collecting information, the agency must tell the individual, and should tell third-party sources, the purposes for which it will be used. This information "should be included on the information collection form, on a tear-off sheet attached to the form, or on a separate sheet which the individual can retain, whichever is most practical." (See item 8 above.) |

C. Disclosure Accounting Features

| | | | |
|---|---|---|---|
| 28956 | 2 | 3(c)(3) | 29. Disclosure accountings must be structured in such a way that the accountings can be retrieved and shown to individuals upon their request. |
| 28956 | 1 | 3(c)(1) | 30. The disclosure accounting records should provide a cross-reference to the justification or basis on which disclosure was made. |
| 28956 | 2 | 3(c)(2) | 31. The disclosure accountings must be retained for at least five years from the date of disclosure or the life of the record disclosed, whichever is longer. |
| 28956<br>28959 | 2 & 3<br>1 | 3(c)(4)<br>3(d)(2)(B) | 32. Agencies must be able to notify past recipients for whom accountings were made about corrections to records they received if the correction request is made by the individual. However, if the correction is a significant change to the record, past recipients should be notified regardless of who initiated the correction. |

II. Administrative Requirements

A. General

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28975 | 3 | 3(m) | 1. Agencies shall cause the provisions of the Act to be applied to systems of records operated by a contractor to accomplish an agency function. (Contractor personnel are considered employees of an agency where criminal penalties are concerned.) |
| 28970 | 2 | 3(i) | |
| 28965 | 3 | 3(e)(9) | 2. Agencies must establish rules of conduct for employees and ensure that contractor employees are fully informed of their obligations when they are subject to the provisions of the Act. |
| -28966 | 1 | | |
| 28970 | 2 | 3(i) | |
| 28976 | 3 | 3(m) | |
| 28965 | 2 - 3 | 3(e)(7) | 3. Information collection may not describe a person's religious or political beliefs or his or her exercise of free speech, press, right to petition government or right to assemble, unless:<br>a. a law specifically authorizes the collection;<br>b. the individual authorizes it; or<br>c. the record is required for an authorized law enforcement function. |
| 28976 | 3 | 3(n) | 4. Agencies may not sell or rent mailing lists for commercial purposes unless specifically authorized by law to do so. |

B. Disclosure Accounting Requriements

| | | | |
|---|---|---|---|
| 28955 | 3 | 3(c) | 5. Record systems must include a disclosure accounting feature although "The agency may use any system it desires for keeping notations of disclosure". |
| -28956 | 1 | | |
| 28955 | 3 | 3(c)(1) | 6. An accounting of disclosures is required:<br>a. For disclosures for routine uses;<br>b. For disclosures to the Bureau of the Census;<br>c. For disclosures to a person or another agency for statistical research or reporting purposes;<br>d. For disclosures to the Archives;<br>e. For disclosures for a law enforcement activity consistent with the provisions of subsection 3(b)(7); |

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| | | | f. For disclosures upon a showing of "compelling circumstances";<br>g. For disclosures to the Congress or the Comptroller General; or<br>h. For disclosures pursuant to a court order.<br><br>An accounting of disclosures is not required:<br><br>a. For disclosures to employees of the agency maintaining the record who have a need to have access in the performance of their official duties for the agency . . .;<br>b. For disclosures which would be required under the Freedom of Information Act. |
| 28956 | 2 | 3(c)(3) | 7. Agencies must be able to make accountings of disclosure available to the individual in a comprehensible form. (It follows from this that if the disclosure accounting is computerized, there ought to be query, retrieval and format routines available to supply information to the individual.) |
| 28956 | 1 | 3(c)(1) | 8. The disclosure accounting system of records is not a system of records for the purposes of the Act. |
| C. Requirements for Granting Access | | | |
| 28956<br>28967 | 3<br>3 | 3(d)<br>3(f)(3) | 9. Agencies must establish procedures granting individuals access to records about themselves. |
| 28957<br>28968 | 1<br>1 | 3(d)(1)<br>3(f)(5) | 10. Agencies may establish fees which represent only the costs of making copies, and not the expenses incurred in searching for and translating records. |
| 28957 | 3 | 3(d)(1) | 11. Agencies will normally provide access to a record within 30 working days. |
| 28957<br>28967 | 2<br>1 | 3(d)(1)<br>3(f)(1) | 12. Agencies may not deny individuals access to records about themselves for refusing to disclose their Social Security Numbers.* |
| 28957<br>28967 | 2 & 3<br>3 | 3(d)(1)<br>3(f)(3) | 13. Agencies may have to establish special procedures for disclosure of medical records. |

*See Comment on Page 4

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| 28957<br>28964<br>28967 | 2<br>2<br>1 | 3(d)(1)<br>3(e)(4)(H)<br>3(f)(1) | 14. The identities of people seeking to gain access to records about themselves must be verified before the information is given to them unless the information would be available to the public under the Freedom of Information Act. Special procedures for verifying identities may have to be established when access is granted by mail. (See also item 17 below). |
| 28957 | 1 | 3(d)(1) | 15. Agencies do not have to grant individuals access to information about themselves when the information sought is in a record about another person if an elaborate cross reference system would have to be developed that would increase the risks of privacy abuse. |
| D. Requirements for Amending Records | | | |
| 28958<br>28967 | 1<br>3 | 3(d)(2)<br>3(f)(4) | 16. The agency must allow individuals to request corrections to records. |
| 28958 | 1 | 3(d)(2) | 17. The identities of individuals seeking to correct records about themselves should be verified to make sure that they are not deliberately or inadvertently seeking to change records about other people. |
| 28958 | 1 | 3(d)(2) | 18. The agency should not categorically reject incomplete or inaccurate requests from people for amending records about themselves. The agency should give the individual the opportunity to submit additional required data. |
| 28959 | 1 | 3(d)(2)(B) | 19. If an agency agrees to amend a record it should:<br>a. Correct the record;<br>b. Advise the individual; and<br>c. Where an accounting of disclosure has been made, advise previous recipients of the correction. |
| 28956 | 3 | 3(c)(4) | 20. The requirement that recipients be notified of corrections to records does not apply to a) personnel within the agency with a 'need to know', or b) to disclosures made to the public under the Freedom of Information Act, or c) to disclosures made before 9/27/75. |

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | |
|---|---|---|---|
| E. Reports and Notices | | | |
| 28962 | 3 | 3(e)(4) | 21. Annual Public Notice: A notice of the existence and character of each personal information system maintained by an agency must be published annually in the Federal Register. For more information see the "Office of the Federal Register Publication Guidelines for the Privacy Act of 1974," Federal Register, June 19, 1975, Vol. 40, No. 119. |
| 28962 | 3 | 3(e)(4) | 22. Guidance is given for determining whether a system is to be treated as one system or several systems of records. "Purpose" is the most important criterion. |
| 28970 | 3 | 3(i)(2) | 23. "The officer or employee who maintains the system has an obligation to notify the one responsible for publishing the notice. Similarly, the officer or employee responsible for publishing the notice, once notified of the existence of a system, must make that fact public." |
| 28966 | 2 - 3 | 3(e)(11) | 24. Notices for New/Revised Routine Uses must be published:<br>a. "For any new systems of records for which routine uses are contemplated;"<br>b. "For an existing system of records whenever a 'new routine' is proposed;"<br>c. "For all existing systems not later than August 28, 1975." |
| 28960 | 3 | 3(e)(1) | 25. The agency must be able to identify the specific provision in law which authorizes a personal data collection activity and should cite that provision in the annual public notice where feasible. |
| 28966<br>28963 | 2<br>3 | 3(e)(11)<br>3(e)(4) | 26. Before a record is disclosed for any particular routine use that routine use must have been published in a Federal Register notice. |
| 28963<br>28977 | 2<br>1 - 3 | 3(e)(4)<br>3(o) | 27. An agency must automatically report to the Privacy Protection Study Commission (PPSC), OMB (Information Systems Division), and Congress whenever it establishes a new system and before changes to existing systems are effective. |
| 28963<br>28963 | 2<br>3 | 3(e)(4)<br>3(e)(4)(B) | 28. Revised public notices must also be published before major changes to existing systems become effective. (Narrowing of coverage does not require advance issuance of a revised public notice.) |

| Page of OMB Guidelines | Column Number | Section of OMB Guidelines | | |
|---|---|---|---|---|
| 28963-<br>28964 | 2 - 3<br>1 - 3 | 3(e)(4)(A) thru<br>3(e)(4)(H) | 29. | For purposes of issuing revised public notices, the following condition constitutes change:<br><br>"Any new use or significant change in an existing system which has the effect of expanding the availability of the information in the system." This type of change would include the following:<br><br>a. any such change in a routine use;<br>b. an expansion of<br><br>1) the categories of records maintained;<br>2) the categories of individuals on whom records are maintained;<br>3) the potential recipients of the information; and<br><br>c. any modification that alters the procedures by which individuals exercise their rights under the Act. |
| 28963 | 3 | 3(e)(4)(C) | 30. | "The addition of a new data element clearly within the scope of the categories in the notice would not require the issuance of a revised notice." |
| 28977 | 2 | 3(o) | 31. | For the purposes of sending reports to OMB, the Privacy Protection Commission and Congress about proposals to alter existing systems, the following conditions constitute change:<br><br>a. An increase in the number or types of individuals on whom records are maintained;<br>b. Expansion of the type or amount of information maintained;<br>c. An increase in the number or categories of agencies or persons who have access to those records;<br>d. Alteration of the manner in which records are organized so as to change the nature or scope of those records--i.e., combining two or more systems;<br>e. Alteration of the way the system operates or its location(s) in a way that the process by which individuals can gain access to, or request changes in, records is changed;<br>f. Change of the equipment configuration in a way that creates potential for greater access, e.g., if add a telecommunications capability. |

NBS-114A (REV. 7-73)

| U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET | 1. PUBLICATION OR REPORT NO. NBS IR-75-909 | 2. Gov't Accession No. | 3. Recipient's Accession No. |
|---|---|---|---|

**4. TITLE AND SUBTITLE**

*Index of Automated System Design Requirements as Derived from the OMB Privacy Act Implementation Guidelines*

**5. Publication Date**
*1975 December 1*

**6. Performing Organization Code**
640.01

**7. AUTHOR(S)**

**8. Performing Organ. Report No.**

**9. PERFORMING ORGANIZATION NAME AND ADDRESS**

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

**10. Project/Task/Work Unit No.**
600 1101

**11. Contract/Grant No.**

**12. Sponsoring Organization Name and Complete Address** *(Street, City, State, ZIP)*

Office of ADP Standards Management
Institute for Computer Sciences and Technology
National Bureau of Standards, Washington, D.C. 20234

**13. Type of Report & Period Covered**
*Final*

**14. Sponsoring Agency Code**

**15. SUPPLEMENTARY NOTES**

**16. ABSTRACT** *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

*This index is a list of certain requirements which must be considered by Federal technical and administrative personnel in order to comply with those provisions of the Privacy Act of 1974* relating to automated systems design and development. This index has been derived from the Office of Management and Budget (OMB) guidelines** for implementing those provisions. Each requirement listed contains a reference to an applicable part of the Privacy Act and to a page and column number of the OMB guidelines as they appear in the Federal Register. Therefore, these documents must be used in conjunction with this index. Furthermore, a familiarity with these documents will increase the utility of this index.*

**17. KEY WORDS** *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

*Computer; data processing; index; information processing; privacy; requirements definition; systems design; security*

**18. AVAILABILITY**

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13

[X] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

**19. SECURITY CLASS (THIS REPORT)**
UNCLASSIFIED

**21. NO. OF PAGES**
14

**20. SECURITY CLASS (THIS PAGE)**
UNCLASSIFIED

**22. Price**
$3.25